How to Remove Lilith RAT: Complete Removal Guide | Trojan Killer

By Gridinsoft Team

Published: 2025-04-06 · Archived: 2026-04-02 12:05:33 UTC

Lilith RAT is an advanced remote access trojan written in C++ programming language that provides attackers with complete control over an infected computer. This malicious tool allows hackers to remotely execute commands, steal sensitive data, and install additional malware. In this guide, we'll examine how Lilith RAT works, its distribution methods, infection symptoms, and provide step-by-step instructions for completely removing this threat.

Key Facts

- **Threat Type:** Remote Access Trojan (RAT), Trojan
- **Affected Platforms:** Windows 7, 8, 8.1, 10, 11
- **Distribution Methods:** Phishing emails, malicious attachments, vulnerability exploits
- **Main Symptoms:** Hidden command execution, data theft, system performance issues
- **Danger Level:** High
- **Potential Damage:** Password and banking information theft, identity theft, additional malware installation
- **Detection Method:** Antivirus scanning, process analysis, network traffic monitoring
- **Year Discovered:** 2022

What is Lilith RAT?

Lilith RAT is a remote access trojan designed to give attackers full control over infected systems. Written in C++, this lightweight yet powerful RAT offers a wide range of features for remote control, data theft, and conducting further attacks.

Unlike less sophisticated trojans, Lilith RAT allows attackers to execute commands remotely using CMD (Command Prompt), PowerShell, or other console-based applications. This gives cybercriminals significant control over the system, allowing them to run scripts, control system functions, or make changes to the infected computer.

Name:	Lilith remote access trojan
Threat Type:	Remote Access Trojan (RAT)
Detection Names:	Avast (LNK:Agent-HN [Trj]), ESET-NOD32 (LNK/Agent.AHE), Kaspersky (HEUR:Trojan.Multi.Agent.gen), Sophos (Troj/LnkDrop-M)

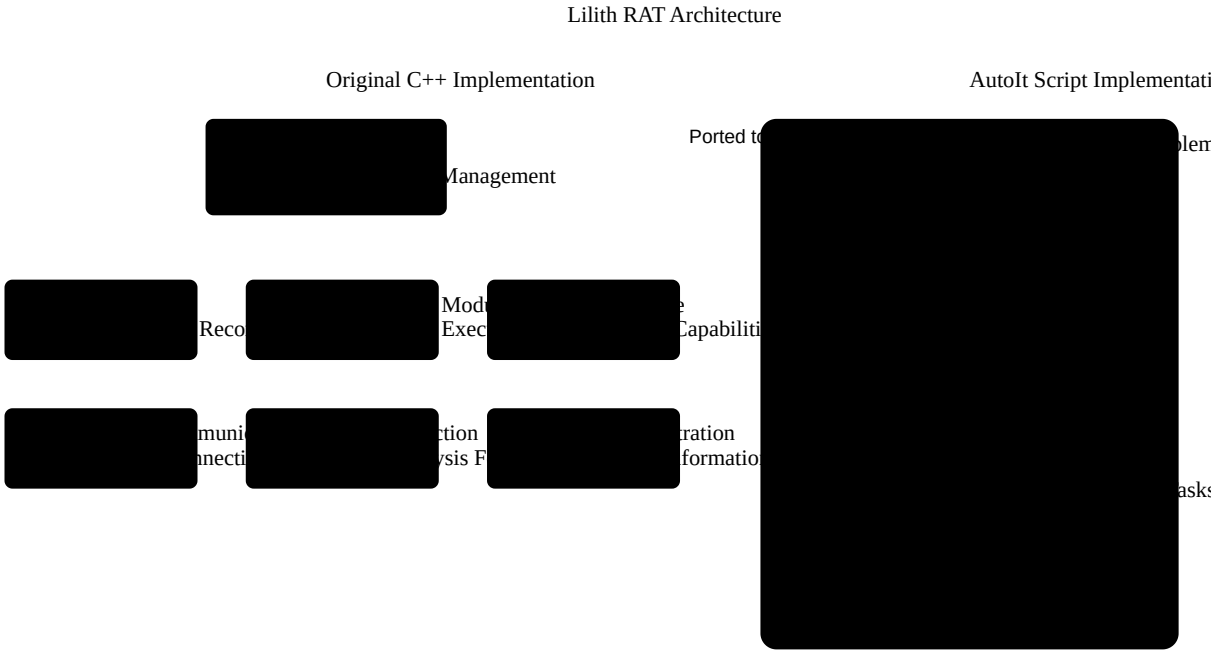
Symptoms:	Remote Access Trojans are designed to stealthily infiltrate the victim's computer and remain silent, and thus no particular symptoms are clearly visible on an infected machine.
Distribution Methods:	Deceptive emails containing malicious files or links, malicious online advertisements, social engineering, pirated software, technical support scam.
Damage:	Stolen passwords and banking information, identity theft, possible additional infections, monetary loss.

Lilith RAT Capabilities

Lilith RAT features a wide range of functions that make it a dangerous threat to users:

- **Remote Command Execution:** Ability to execute commands through CMD, PowerShell, and other console applications
- **Keylogger:** Records everything the victim types, including passwords, messages, and bank card data
- **Mass Control:** Sending a single command to all infected devices simultaneously
- **Auto-start:** Installation without additional input from attackers and automatic execution at every computer startup
- **Self-destruction:** Ability to delete its own files to cover tracks
- **Error Analysis:** Finding and logging errors to track functionality issues

Architecture and Technical Characteristics of Lilith RAT



Modular architecture of Lilith RAT, showing the original C++ implementation and the AutoIt variant used by the puNK-003 group from North Korea

How is Lilith RAT Distributed?

Cybercriminals distribute Lilith RAT primarily through targeted phishing attacks. A typical scenario involves sending emails with malicious attachments or links. These attacks usually use an LNK file (shortcut) disguised as a document. When the LNK file is opened, it displays a fake document and downloads files from an attacker’s server. These files include a malicious AutoIt script that launches the Lilith RAT malware.

In 2024, security researchers identified a North Korean threat actor group dubbed “puNK-003” using Windows shortcut (LNK) files to distribute a variant of Lilith RAT. This distribution method, named “CURKON” by researchers, acts as a downloader that retrieves AutoIt scripts from the attacker’s server. The original C++ implementation of Lilith RAT has been ported to AutoIt script language, allowing attackers to maintain the same functionality while evading traditional detection methods.

Lilith RAT Infection Process

North Korean Threat Actor: puNK-003

In 2024, security researchers identified a specific variant of Lilith RAT being distributed by a North Korean APT (Advanced Persistent Threat) group named puNK-003. This group has shown connections to the well-known KONNI threat actor, though with some distinct operational differences.

The puNK-003 attack chain works as follows:

1. Distribution of malicious LNK files (named “CURKON” by researchers) disguised as tax-related documents
2. When executed, the LNK file drops a decoy document while downloading additional files
3. The malware creates a hidden folder on the C drive and copies the legitimate curl.exe utility
4. Using curl, it downloads both AutoIt3.exe (a legitimate interpreter) and a malicious AutoIt script
5. The downloaded script is a recreation of Lilith RAT, ported from C++ to AutoIt
6. For persistence, the malware creates scheduled tasks to ensure it runs every few minutes

Technical Details of AutoIt Implementation

The AutoIt implementation of Lilith RAT created by puNK-003 differs from the original C++ version in several ways:

- It maintains primary functionalities but with a simpler structure
- It uses a mutex named “Global\RT3AN7C9QS-7UYE-9K6G-A8F1-HY8IT3CNMEQP” to prevent multiple instances
- It checks for specific antivirus products (particularly Avast) and adjusts its behavior accordingly

- It implements a simplified reverse shell functionality for command execution
- It communicates with hardcoded C2 servers on non-standard ports (e.g., 57860)

Technical Indicators of Compromise (IoCs)

Indicator Type	Value	Notes
File	LNK files with random names	Usually disguised as Office documents or PDFs
Process	Random process names, autostart	Often uses code injection into legitimate processes
Registry	Autostart entries in HKCU\Software\Microsoft\Windows\CurrentVersion\Run	Used for persistence
Network Activity	Unusual outbound traffic to unknown domains	Communication with command and control (C&C) servers
File Hashes (CURKON)	9d6c79c0b395cceb83662aa3f7ed0123 2189aa5be8a01bc29a314c3c3803c2b8131f49a84527c6b0a710b50df661575e 3334d2605c0df26536058f73a43cb074	LNK files used in puNK-003 campaigns
File Hashes (AutoIt Script)	5613ba2032bc1528991b583e17bad59a 808425bc599cd60989c90978d179af1d4c72dd7abfe5e0518aca44b48af15725 d5809e5f848f228634aa45ffe4a5ece0	AutoIt script implementation of Lilith RAT
C2 Servers	93.183.93[.]185:57860 185.231.154[.]22:52720 62.113.118[.]157:57860	Command and control servers used by puNK-003
Symantec Detections	ACM.Ps-Rd32!g1, ACM.Ps-RgPst!g1, ACM.Ps-Schtsk!g1, ACM.Ps-SvcReg!g1, CL.Downloader!gen20, CL.Downloader!gen204, Scr.Mallnk!gen13, Trojan.Gen.NPE	Detection signatures for the puNK-003 variant

Signs of Lilith RAT Infection

Since Lilith RAT is designed for stealthy operation, determining its presence in a system can be difficult. Nevertheless, there are certain signs that may indicate infection:

- **Unexplained system activity:** High processor or network usage when no programs are running
- **Unusual network activity:** Outbound connections to unknown IP addresses or domains
- **Strange computer behavior:** Programs or windows opening/closing spontaneously
- **Disabled protection mechanisms:** Antivirus software or firewall shutting down without your knowledge
- **Unexpected privilege elevation requests:** System notifications about access requests from unknown programs
- **Account issues:** Unexplained logins to your online accounts or changes to them
- **Strange processes in Task Manager:** Unusual or suspicious processes with random names

Threats and Potential Damage from Lilith RAT

Lilith RAT poses a serious security threat that can lead to significant damage:

- **Theft of confidential information:** Passwords, financial data, personal information
- **Financial losses:** Access to bank accounts and credit cards
- **Identity theft:** Use of personal data for fraud or other crimes
- **Espionage:** Monitoring all user activities, including correspondence and communication
- **Additional infections:** Installation of ransomware or other malware
- **Remote control:** Complete control over the computer without the owner’s knowledge
- **Corporate espionage:** In case of infection of work computers – access to corporate information

The process of removing Lilith RAT requires a comprehensive approach due to the complexity and stealth of this threat. Below are methods for removing the malware.

Method 1: Removal Using Trojan Killer

For effective removal of Lilith RAT, it is recommended to use specialized antivirus software, such as Trojan Killer:

1. **Download and install Trojan Killer** from the official website
2. **Run a full system scan**:
    - Launch the program with administrator privileges
    - Select the full scan option
    - Wait for the process to complete (may take 20-40 minutes depending on the system)
3. **Review scan results**:
    - The program will display a list of detected threats
    - Make sure all Lilith RAT components are selected for removal
4. **Remove detected threats**:
    - Click the “Remove Selected” button
    - Follow the program instructions to complete the removal process
5. **Restart your computer** to complete the removal process
6. **Perform a second scan** to verify complete removal of the threat

Method 2: Manual Removal (for Advanced Users)

Warning: Manual removal of Lilith RAT requires technical knowledge and experience. Incorrect actions may damage the operating system. This method is recommended only for experienced users.

1. **Boot the computer in Safe Mode with Networking**:
    - Restart the computer
    - During startup, press F8 (or Shift+F8 in Windows 10)
    - Select “Safe Mode with Networking”

2. **Open Task Manager and terminate suspicious processes**:
    - Press Ctrl+Shift+Esc to open Task Manager
    - Look for processes with unusual or random names
    - For each suspicious process: select it and click “End Process”
3. **Check startup items and remove suspicious elements**:
    - Press Win+R, type “msconfig” and press Enter
    - Go to the “Startup” tab (depending on Windows version)
    - Disable all suspicious items
4. **Check the Task Scheduler**:
    - Press Win+R, type “taskschd.msc” and press Enter
    - Review scheduled tasks and delete suspicious ones
5. **Clean the registry**:
    - Press Win+R, type “regedit” and press Enter
    - Check the following registry sections:
        - HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run
        - HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run
        - HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce
        - HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunOnce
    - Delete suspicious entries
6. **Remove malicious files**:
    - Check the following folders:
        - C:\Windows\Temp\
        - C:\Users\[username]\AppData\Local\Temp\
        - C:\Users\[username]\AppData\Roaming\
        - C:\ProgramData\
    - Delete suspicious files and folders
7. **Restart the computer in normal mode**
8. **Change all passwords** for important accounts from another, uninfected device

Method 3: System Restore

If the Lilith RAT infection occurred recently, you can try restoring the system to a point before the infection:

1. **Open System Restore**:
    - Press Win+R
    - Type “rstrui.exe” and press Enter
2. **Select a restore point**:
    - Choose a restore point created before the infection
    - Follow the wizard instructions to complete the process
3. **After system restoration**, it is still recommended to perform a full antivirus scan

Advanced Technical Analysis For Security Researchers

The puNK-003 variant of Lilith RAT represents a significant evolution in the threat landscape, showing how North Korean APT actors are adapting and repurposing existing malware tools. This section provides a detailed analysis specifically for security professionals and threat hunters.

North Korean puNK-003 Implementation

In 2024, researchers identified a previously unknown North Korean threat actor group (dubbed “puNK-003”) using Windows shortcut (LNK) files to distribute a variant of Lilith RAT. Unlike the original C++ implementation, this variant has been completely ported to AutoIt scripting language, providing several advantages:

- Bypass of signature-based detection that targets the original C++ binary
- Execution through a legitimate interpreter (AutoIt3.exe), which appears less suspicious
- Easier modification and customization of functionality
- Simplified evasion of memory scanning techniques that target C/C++ patterns

AutoIt Script Analysis

The AutoIt implementation shows evidence of careful manual conversion rather than automated translation, with several functions recreated to achieve similar results through different means:

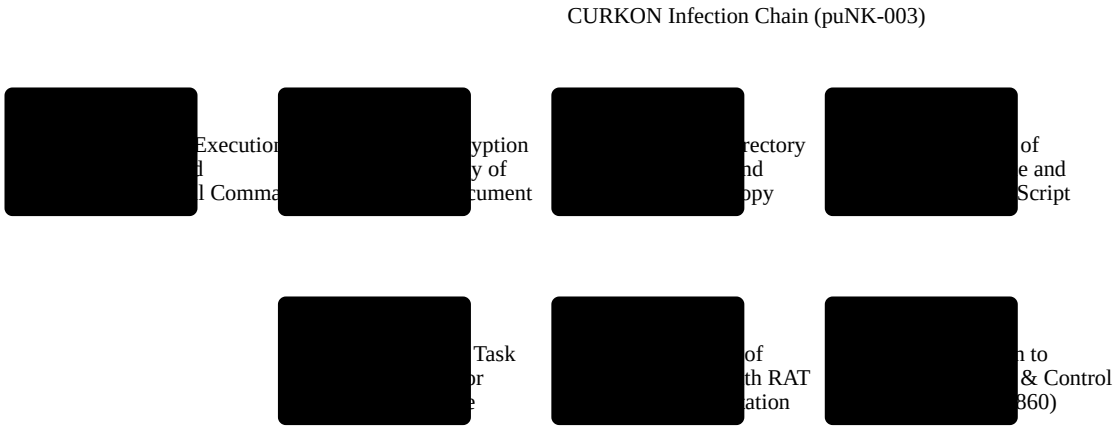
```
; Example from AutoIt implementation of Lilith RAT

Func ISMULTIPLE()

    Local $mutex = "Global\RT3AN7C9QS-7UYE-9K6G-A8F1-HY8IT3CNMEQP"

    Local $handle = DllCall("kernel32.dll", "handle", "CreateMutexA", "ptr", 0, "bool", True, "str", $mutex)

    If @error Then Return False

    Local $lastError = DllCall("kernel32.dll", "dword", "GetLastError")

    If $lastError[0] = 183 Then ; ERROR_ALREADY_EXISTS

        Return True

    EndIf

    Return False

EndFunc
```

Initial Infection Vector (CURKON)

The initial infection vector, named CURKON, is a specially crafted LNK file that executes PowerShell commands when opened. Analysis of these LNK files reveals sophisticated techniques including:

- Obfuscation of PowerShell commands using string manipulation and logical operators

- XOR operations with a hardcoded one-byte key (0xD8) for decryption
- Dropping and executing decoy documents to maintain the illusion of legitimacy
- Creating hidden directories with specific naming patterns (e.g., “GSlLzFnTov”)
- Using legitimate Windows utilities (curl.exe) for secondary payload download



Full infection chain for CURKON/Lilith RAT deployment by puNK-003

Command and Control Infrastructure

The C2 infrastructure used by puNK-003 shows several distinctive characteristics:

- Primary use of compromised WordPress websites as first-stage C2 servers
- Secondary communication with dedicated IP addresses on non-standard ports
- Specific URL patterns in WordPress sites, typically using paths like “/wp-admin/css/temp/”
- Query string parameters that follow predictable patterns (e.g., “?rv=papago&za=honey0”)

Technical Comparison: Original vs AutoIt Implementation

The table below compares key features between the original C++ Lilith RAT and the AutoIt implementation used by puNK-003:

Feature	Original C++ Implementation	puNK-003 AutoIt Implementation
File Size	~300KB compiled binary	~40KB script + ~800KB AutoIt3.exe interpreter
Keylogging	Full implementation with keystroke recording	Limited implementation, focused on specific inputs
Remote Command Execution	Comprehensive with multiple shell options	Limited to cmd.exe and powershell.exe

Anti-Analysis	Multiple checks for VMs, debuggers	Limited to security software checks (Avast)
Persistence	Registry and startup folder	Primarily scheduled tasks
C2 Protocol	Custom binary protocol	Simplified text-based communication

MITRE ATT&CK Mapping

The puNK-003 implementation of Lilith RAT employs the following key MITRE ATT&CK techniques:

- **T1566.001:** Phishing: Spearphishing Attachment – Distribution of LNK files disguised as documents
- **T1059.001:** Command and Scripting Interpreter: PowerShell – Execution of obfuscated commands
- **T1059.005:** Command and Scripting Interpreter: Visual Basic – Use of AutoIt scripting
- **T1053.005:** Scheduled Task/Job: Scheduled Task – Creation of tasks running every 1-10 minutes
- **T1564.001:** Hide Artifacts: Hidden Files and Directories – Creation of hidden folders
- **T1140:** Deobfuscate/Decode Files or Information – XOR decryption of embedded payloads
- **T1571:** Non-Standard Port – Use of uncommon ports like 57860 for C2 communication
- **T1518.001:** Software Discovery: Security Software Discovery – Checks for Avast products

Attribution Evidence

Evidence linking the puNK-003 group to North Korean threat actors includes:

- Code similarities with KONNI group implementations, particularly in the ISMULTIPLE() function
- Infrastructure patterns consistent with other North Korean operations
- Similar LNK file obfuscation techniques to those used by other North Korean threat actors
- Targeting patterns aligned with North Korean strategic interests

However, distinct differences from the KONNI group include:

- puNK-003 uses CURKON primarily as a downloader, while KONNI's LINKON acts as a dropper
- puNK-003 campaigns lack the VBS and BAT scripts commonly used in KONNI operations
- Different approaches to persistence and system manipulation

Detection Strategies

Key strategies for detecting this variant include:

1. **LNK File Analysis:** Monitor for LNK files with obfuscated PowerShell commands
2. **PowerShell Command Detection:** Look for scripts with encoding bypass parameters and XOR operations
3. **Filesystem Monitoring:** Watch for hidden directories and copied system utilities (curl.exe)
4. **Network Traffic Analysis:** Monitor for connections to WordPress sites with specific patterns and non-standard ports
5. **Behavioral Analysis:** Detection of scheduled tasks with short intervals and mutex creation

YARA Rule for Detection

The following YARA rule (in YAML syntax) can help detect the AutoIt implementation of Lilith RAT:

```
---
rule: LilithRAT_AutoIt_puNK003
meta:
    description: "Detects puNK-003's AutoIt implementation of Lilith RAT"
    author: "Trojan Killer Research Team"
    date: "2025-04"
    hash1: "5613ba2032bc1528991b583e17bad59a"
    severity: "high"
strings:
    mutex: "Global\\RT3AN7C9QS-7UYE-9K6G-A8F1-HY8IT3CNMEQP ascii wide"
    autoit1: "#include < ascii"
    autoit2: "Func ascii"
    autoit3: "EndFunc ascii"
    func1: "ISMULTIPLE ascii nocase"
    func2: "CheckAV ascii nocase"
    av1: "AvastUI.exe ascii wide"
    av2: "AvastSvc.exe ascii wide"
    net1: "TCPConnect ascii"
    net2: ":57860 ascii wide"
condition: >
    (2 of ($autoit*)) and
    (
      $mutex or
      (1 of ($func*) and 1 of ($av*)) or
```

```
    (1 of ($av*) and 1 of ($net*))
)
```

Signs of Lilith RAT Infection

Since Lilith RAT is designed for stealthy operation, determining its presence in a system can be difficult. Nevertheless, there are certain signs that may indicate infection:

- **Unexplained system activity:** High processor or network usage when no programs are running
- **Unusual network activity:** Outbound connections to unknown IP addresses or domains
- **Strange computer behavior:** Programs or windows opening/closing spontaneously
- **Disabled protection mechanisms:** Antivirus software or firewall shutting down without your knowledge
- **Unexpected privilege elevation requests:** System notifications about access requests from unknown programs
- **Account issues:** Unexplained logins to your online accounts or changes to them
- **Strange processes in Task Manager:** Unusual or suspicious processes with random names

Threats and Potential Damage from Lilith RAT

Lilith RAT poses a serious security threat that can lead to significant damage:

- **Theft of confidential information:** Passwords, financial data, personal information
- **Financial losses:** Access to bank accounts and credit cards
- **Identity theft:** Use of personal data for fraud or other crimes
- **Espionage:** Monitoring all user activities, including correspondence and communication
- **Additional infections:** Installation of ransomware or other malware
- **Remote control:** Complete control over the computer without the owner’s knowledge
- **Corporate espionage:** In case of infection of work computers – access to corporate information

How to Remove Lilith RAT

The process of removing Lilith RAT requires a comprehensive approach due to the complexity and stealth of this threat. Below are methods for removing the malware.

Method 1: Removal Using Trojan Killer

For effective removal of Lilith RAT, it is recommended to use specialized antivirus software, such as Trojan Killer:

1. **Download and install Trojan Killer** from the official website
2. **Run a full system scan**:
    - Launch the program with administrator privileges
    - Select the full scan option
    - Wait for the process to complete (may take 20-40 minutes depending on the system)
3. **Review scan results**:
    - The program will display a list of detected threats
    - Make sure all Lilith RAT components are selected for removal
4. **Remove detected threats**:
    - Click the “Remove Selected” button
    - Follow the program instructions to complete the removal process
5. **Restart your computer** to complete the removal process
6. **Perform a second scan** to verify complete removal of the threat

Method 2: Manual Removal (for Advanced Users)

Warning: Manual removal of Lilith RAT requires technical knowledge and experience. Incorrect actions may damage the operating system. This method is recommended only for experienced users.

1. **Boot the computer in Safe Mode with Networking**:
    - Restart the computer
    - During startup, press F8 (or Shift+F8 in Windows 10)
    - Select “Safe Mode with Networking”

2. **Open Task Manager and terminate suspicious processes**:
    - Press Ctrl+Shift+Esc to open Task Manager
    - Look for processes with unusual or random names
    - For each suspicious process: select it and click “End Process”
3. **Check startup items and remove suspicious elements**:
    - Press Win+R, type “msconfig” and press Enter
    - Go to the “Startup” tab (depending on Windows version)
    - Disable all suspicious items
4. **Check the Task Scheduler**:
    - Press Win+R, type “taskschd.msc” and press Enter
    - Review scheduled tasks and delete suspicious ones
5. **Clean the registry**:
    - Press Win+R, type “regedit” and press Enter
    - Check the following registry sections:
        - HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run
        - HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run
        - HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce
        - HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunOnce
    - Delete suspicious entries
6. **Remove malicious files**:
    - Check the following folders:
        - C:\Windows\Temp\
        - C:\Users\[username]\AppData\Local\Temp\
        - C:\Users\[username]\AppData\Roaming\
        - C:\ProgramData\
    - Delete suspicious files and folders
7. **Restart the computer in normal mode**
8. **Change all passwords** for important accounts from another, uninfected device

Method 3: System Restore

If the Lilith RAT infection occurred recently, you can try restoring the system to a point before the infection:

1. **Open System Restore**:
    - Press Win+R
    - Type “rstrui.exe” and press Enter
2. **Select a restore point**:
    - Choose a restore point created before the infection
    - Follow the wizard instructions to complete the process
3. **After system restoration**, it is still recommended to perform a full antivirus scan

Conclusion

Lilith RAT represents a serious cybersecurity threat, providing attackers with extensive capabilities to control infected systems, steal confidential information, and conduct further attacks. Its stealthy nature and advanced features make it particularly dangerous for both regular users and organizations.

Effective protection against Lilith RAT and similar threats requires a comprehensive approach to security, including the use of antivirus software, regular software updates, caution when working with email, and general cyber hygiene. When infection is detected, it's important to act quickly, using reliable tools to remove the threat and minimize potential damage.

For the most effective removal of Lilith RAT, it is recommended to use specialized antivirus software such as Trojan Killer, which can detect and remove this complex threat, even when it tries to hide from standard security solutions.
